IN THE UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF MISSISSIPPI, NORTHERN DIVISION

EMMA G. MICHAEL,	**PLAINTIFF**
VS.	**CASE NO.** 3:15cv72 HTW-LRA **CLASS ACTION COMPLAINT**
VERIZON COMMUNICATIONS, INC.; CELLCO PARTNERSHIP d/b/a VERIZON WIRELESS; VERIZON WIRELESS, LLC; TURN, INC.	**DEFENDANTS**

CLASS ACTION COMPLAINT

Plaintiff, Emma G. Michael, on behalf of herself and all others similarly situated, by and through their attorneys, Bradley S. Clanton and Clanton Legal Group, PLLC, and for their Complaint allege as follows upon information and belief, based upon, inter alia, investigation conducted by and through their attorneys, which are alleged upon knowledge, and sue Defendants Verizon Communications, Inc., Cellco Partnership d/b/a/ Verizon Wireless, and Verizon Wireless, LLC (collectively referred to herein as "Verizon"), and Turn, Inc. Plaintiff's

upon her personal knowledge, and all other allegations are based upon information and belief pursuant to the investigation of counsel. Based upon such investigation, Plaintiff and Class Members believe that substantial evidentiary support exists for the allegations herein or that such allegations are likely to have evidentiary support after a reasonable opportunity for further investigation and/or discovery.

II. Introduction and Background

A. Nature of the Case

1. Plaintiff brings this consumer class action lawsuit pursuant to Federal Rules of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3), on behalf of herself and all other members of a class of similarly-situated internet users, hereinafter referred to as the "Class Members," who were victims of unfair, deceptive, and unlawful business practices, wherein their privacy, financial interests, and computer security rights, were violated by Verizon, and websites affiliated individually with Verizon, referred collectively to as, "Verizon Supercookie Affiliates," and individually, Turn Inc., by injecting permanent "supercookies" onto user's computers to track, store, transmit and/or use data regarding the users' browsing history and other sensitive personal and confidential information.

2. Verizon Supercookie Affiliates, and Turn, acted with Verizon, independent of one another, and knowingly authorized, directed, ratified, approved, acquiesced, or participated in the unfair and deceptive business practices made the basis of this class action, which included, but were not limited to, setting of an online tracking device which would allow access to, and disclosure of, personal information ("PI"), personal identifying information ("PII"), and/or sensitive indentifying information ("SII"). This information was derived from the internet user's online activities, accomplished covertly, without actual notice, awareness, consent or choice of the user, obtained deceptively, for purposes not disclosed within their Terms of Service and/or Privacy Policy and used for commercial gain and nefarious purposes.

3. The conduct of Verizon, individually and in concert with the Verizon Supercookie Affiliates, and Turn, individually and jointly, is an unfair and deceptive practice that has been perpetrated for years, facilitated, and coordinated, by some of the world's largest websites and the network advertising industry, thereby causing the Plaintiff and Class Members significant harm.

4. Defendants, collectively, have been systematically engaged in

and facilitated a covert operation of surveillance of Plaintiff and Class Members and violating one (1) or more of the following:

a. Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (the "CFAA");

b. Electronic Communications Privacy Act, 18 U.S.C. § 2510 (the "ECPA");

c. Video Privacy Protection Act, 18 U.S.C. § 2710, (the "VPPA");

d. Unjust Enrichment, fraud, and other common law torts.

B. The Parties

5. Plaintiff Emma G. Michael, is a resident of Jackson, Mississippi, and has been a Verizon customer for over two decades. She currently has three phones and one keypad providing Verizon internet browsing services, which includes the surreptitious tracking of internet and other activity that is the subject of this Complaint.

6. Defendant Verizon Communications, Inc. is a Delaware corporation doing business in Mississippi with its principal place of business in New York, New York, and may be served with process at its corporate headquarters located at 140 West Street, New York, New York 10007.

7. Defendant Cellco Partnership d/b/a Verizon Wireless is a New Jersey entity doing business in Mississippi and may be served with process at the office of its registered agent, CT Corporation Services, 645 Lakeland East Drive, Suite 101, Flowood, Mississippi 39232.

8. Verizon Wireless, LLC is a Delaware corporation doing business in Mississippi and may be served with process at the office of its registered agent, CT Corporation Services, 645 Lakeland East Drive, Suite 101, Flowood, Mississippi 39232.

9. Defendant Turn, Inc is a California corporation with its principal place of business located at Turn Inc., 835 Main St., Redwood City, California 94063-1901

C. Subject-Matter Jurisdiction

10. This Court has subject-matter jurisdiction over the this matter pursuant to Title 28, United States Code, Section 1332, as amended by the Class Action Fairness Act of 2005, in that (a) the aggregate claims of Plaintiff and the proposed Class Members exceed the sum or value of $5,000,000, exclusive of interest and costs; (b) minimal diversity of citizenship exists between the proposed Class Members and

Defendant; and (c) the Classes each consist of more than one hundred members.

11. This Court has subject-matter jurisdiction over this action pursuant to Title 28, United States Code, Section 1331, as this action arises in part under a federal statute.

12. This Court has supplemental jurisdiction with respect to the pendent state law claims under Title 28, United States Code, Section 1367.

13. Venue is proper in this District under Title 28, United States Code, Section 1391(b), because Defendant's improper conduct alleged in this complaint occurred in, was directed from, and/or emanated from this judicial district.

II. Factual Allegations

A. The Evolution of the Cookie and Supercookie

14. The complexities of the rapidly-exploding and sometimes colliding worlds of wireless connectivity, mobile device prevalence, privacy, and pervasive data farming are mind-boggling.

15. In this case, it all started with "cookies." Cookies are small files which are stored on a user's computer. Cookies allow a website to

use a consumer's internet connection, browser software, and computer processing and storage to create and read data of its own choosing on a computer whenever the consumer downloads a web page. As the use of cookies has become more widespread and well known, their use has fallen into disfavor and has been replaced or supplemented by the use of more permanent "supercookies" which are extraordinarily difficult to remove from users' computers.

16. In the context of the online tracking and trafficking ecosystem, a consumer's ability to use or rely on browser controls to block and delete browser cookies is critical, particularly because: (a) online tracking is invisible, pervasive, and is not typically disclosed adequately; (b) trafficking in data collected from consumers, including personally identifiable information, is invisible and pervasive; (c) online tracking and trafficking depends on the invisible use of the computers, software, and connectivity of consumers such as Plaintiff and Class Members; and (d) Plaintiff's and Class Members' ability to block or delete browser cookies is the most effective option available to consumers for controlling tracking across their web-browsing activities.

17. The ability to use and rely on their browser controls to block and delete browser cookies is material to Plaintiff and Class Members in protecting their privacy interests online and keeping their computers, software, and connectivity from being used to diminish and invade those interests.

18. Plaintiff and Class Members value their privacy while Web-browsing.

19. Plaintiff and Class Members have a reasonable expectation of privacy while Web browsing.

20. Plaintiff and Class Members do not consent to be tracked online in unreasonable and unexpected ways.

21. The information Plaintiff and Class Members disclose incident to intended communications remains an asset they own. Third parties have no right of access of this information for further dissemination. Plaintiff and Class Members believe their computers, Internet connectivity, and software installed on their computers ("Computer Assets") are theirs to use and control, to preserve privacy interests and for other reasons, such as preventing unwanted communications from diminishing value of their Computer Assets.

B. The Supercookie X-UIDH (Or, Your Mobile Device May Be Following You Whether You Like it or Not)

22. In a report published recently by the well-respected Electronic Frontier Foundation ("EFF") entitled "Verizon Injecting Perma-Cookies to Track Mobile Customers, Bypassing Privacy Controls" (Jacob Hoffman-Andrews Nov. 3, 2014), many if not most of the key facts in this case are clearly presented. With liberty, the report is quoted here to describe for the Court the series of events which has led us to this new pinnacle of "big data":

> Verizon Wireless has been silently modifying its users' web traffic on its network to inject a cookie-like tracker. This tracker, included in an HTTP header called X-UIDH, is sent to every unencrypted website a Verizon customer visits from a mobile device. It allows third-party advertisers and websites to assemble a deep, permanent profile of visitors' web browsing habits without their consent.
>
> Verizon apparently created this mechanism to expand their advertising programs, but it has privacy implications far beyond those programs. Indeed, while we're concerned about Verizon's own use of the header, we're even more worried about what it allows others to find out about Verizon users. The X-UIDH header effectively reinvents the cookie, but does so in a way that is shockingly insecure and dangerous to your privacy. Worse still, Verizon doesn't let users turn off this "feature." In fact, it functions even if you use a private browsing mode or clear your cookies. You can test whether the header is injected in your traffic by visiting lessonslearned.org/sniff or amibeingtracked.com over a cell data connection.

How X-UIDH Works, and Why It's a Problem

Like a cookie, this header uniquely identifies users to the websites they visit. Verizon adds the header at the network level, between the user's device and the servers with which the user interacts. Unlike a cookie, the header is tied to a data plan, so anyone who browses the web through a hotspot, or shares a computer that uses cellular data, gets the same X-UIDH header as everyone else using that hotspot or computer. That means advertisers may build a profile that reveals private browsing activity to coworkers, friends, or family through targeted advertising.

Also unlike a cookie, Verizon's header is nearly invisible to the user and can't be seen or changed in the device's browser settings. If a user clears their cookies, the X-UIDH header remains unchanged. Worse, ad networks can immediately assign new cookies and link them to the cleared cookies using the unchanged X-UIDH value. We don't know which data brokers and ad networks are using the header to create behavioral profiles, but Cory Dunne found at least one GitHub repository contained code to extract the header value, as of October 27. The repository has since been quietly deleted but can be viewed at the Internet Archive. Twitter's mobile advertising division also appears to use the header for ad auctions.

Besides cookie clearing, the X-UIDH header bypasses several other built-in browser privacy mechanisms. Cookies belong to a single website and aren't shared with other websites. But one unique X-UIDH header value is shared with all unencrypted websites a user visits, making it easier for ad networks to track that user across many sites in a way not possible with cookies alone. Browsers provide Incognito Mode or Private Browsing Mode in order to defeat some kinds of tracking, but the X-UIDH header, since it is injected at the network layer, ignores those modes. Verizon also chooses to

ignore Do Not Track, a setting users enable in their browser to indicate they do not want to be tracked. Similarly, disabling third-party cookies in browser settings does nothing to stop the X-UIDH header.

To compound the problem, the header also affects more than just web browsers. Mobile apps that send HTTP requests will also have the header inserted. This means that users' behavior in apps can be correlated with their behavior on the web, which would be difficult or impossible without the header. Verizon describes this as a key benefit of using their system. But Verizon bypasses the 'Limit Ad Tracking' settings in iOS and Android that are specifically intended to limit abuse of unique identifiers by mobile apps. Because the header is injected at the network level, Verizon can add it to anyone using their towers, even those who aren't Verizon customers. Notably, Verizon appears to inject the X-UIDH header even for customers of Straight Talk, a mobile network reseller (known as a MVNO) that uses Verizon's network. Customers of Straight Talk don't necessarily have a relationship with Verizon. But according to AdAge, "Corporate and government subscribers are excluded from the new marketing solution."

. . .

Verizon's Claimed Protections

Verizon does provide a sort of limited opt-out for individual customers, but it appears that the opt-out does not actually disable the header. Instead, it merely tells Verizon not to share detailed demographic information with advertisers who present a UIDH value. Meaningful protection from tracking by third parties would require Verizon to omit the header entirely. According to Verizon, the header value is a salted hash, and the hash changes on an undisclosed frequency. However, it's easy for third-party ad networks to create a continuous profile by associating old and new X-UIDH values through their own identifier cookie. Verizon has

> refused to say what identifier they hash to create the identifier, but their recent patent suggests hashing a phone number. If they are indeed hashing phone numbers, it would be a major cryptographic mistake. Phone numbers can easily be deduced from hashes, so sending those hashes to untrusted web sites is practically equivalent to giving them your phone number. Besides the ad networks, the unique X-UIDH header is a boon to eavesdroppers.
>
> We have seen that the NSA uses similar identifying metadata as 'selectors' to collect all of a single person's Internet activity. They also have been shown to use selectors to choose targets for delivering malware via QUANTUMINSERT and similar programs. Having all Verizon mobile users' web traffic marked with a persistent, unique identifier makes it trivial for anyone passively eavesdropping on the Internet to associate that traffic with the individual user in a way not possible with IP addresses alone.
>
> According to Verizon, it began the Precision Market Insights program in 2012, but has consistently refused to provide technical details about how the program worked. The injection of the X-UIDH header went largely unremarked by the technical community until recently because it is so hard to observe. The header is inserted in requests after they leave the phone, so customers cannot detect it using only a phone. In order to detect it, a user needs to run a web server configured to log or echo all HTTP headers, which is very rare.

23. These findings were subsequently confirmed by Jonathan Mayer, a Stanford professor of law and computer science, in "The Turn-Verizon Zombie Cookie," *Web Policy*, Jan. 15, 2015

(http://webpolicy.org/2015/01/14/turn-verizon-zombie-cookie/) (last visited Feb. 4, 2015).

24. Plaintiff and Class Members believe online parties with whom they have not chosen or consented to communicate have no right to access or use Plaintiff or Class Members' Computer Assets.

25. Plaintiff's and Class Members' ability to block and/or delete browser cookies is material to them in protecting their privacy interests; preventing their Computer Assets from being used in ways Plaintiff's and Class Members' do not consent to their being used; and preventing the diminishment and/or invasion of their privacy interests.

26. To avoid being tracked online, Plaintiff and Class Members have used and relied on their browser controls to block and/or delete browser cookies.

27. In addition, Plaintiff and Class Members do not and did not expect their identifiable video selections on the internet to be shared with any third party without their consent.

28. Plaintiff and Class Members reasonably believed that they could rely on their browser settings to control cookies.

29. Plaintiff and Class Members are Verizon consumers in the U.S. consumer who have used the Internet on a mobile or other device with service provide by Verizon during the Class Period.

30. Plaintiff and Class Members did not expect, receive notice of, or consent to the installation of any supercookies and did not want such objects to be installed on their computers for tracking purposes.

31. Plaintiff and Class Members consider information about their online activities to be confidential information that are to be protected from disclosure by periodically deleting cookie.

32. Plaintiff and Class Members consider information about any website they have visited to be in the nature of confidential information that they do not expect to be available to an unaffiliated website from a different domain.

33. Plaintiff and Class Members did not expect, receive notice of, or consent to Defendants' tracking on their computers.

34. Defendants were not authorized to circumvent user controls and commandeer user resources.

35. Defendants' actions in depositing supercookies on Plaintiff's and Class Members' computers, in addition to circumventing Plaintiff's and Class Members' browser controls, affected Plaintiff's and Class Members' reasonable expectations regarding their abilities to control third-party monitoring and information collection in that: (a) many consumers are aware of browser cookies but are unaware of supercookies; (b) consumers' browsers are generally equipped with utilities identifying and controlling third-party browser cookies but consumers but have no reasonable means of identifying or managing supercookies, particularly those repurposed by third-party advertising networks of whose presence consumers are unlikely to be aware.

36. Defendants' actions in depositing and using supercookies were surreptitious and without notice and so were conducted without authorization and exceeding authorization.

37. Plaintiff and Class Members sought to maintain the secrecy and confidentiality of their personal information assets acquired by Defendant.

38. The confidential character of Plaintiff's and Class Members' personal information is further demonstrated by their utilization of browser privacy controls and their reasonable reliance on global standards that protect users from cross-domain activity.

39. The confidential character of Plaintiff's and Class Members' personal information is further demonstrated by Defendants' use of surreptitious and deceptive methods to deposit supercookies on Plaintiff's and Class Members' computers. Defendants have misappropriated Plaintiff's and Class Members' personal information.

C. Harm

40. Consumers routinely engage in online economic exchanges with the websites they visit by exchanging their personal information for the websites' content and services, thereby reducing the costs consumers would otherwise have to pay.

41. Even when such transactions do not involve the transmission of personally identifiable information, but merely *personal* information with which consumers are tracked in supposed anonymity, consumers engage in value-for-value exchanges by providing their information in exchange for content and services.

42. This value-for-value exchange takes place particularly when a website's offerings are supported by advertising revenue. In such cases, the consumer becomes a participant in what is known as a two-sided business platform. On one side is one customer (the consumer), and on the other side is the advertiser. The website stands in middle as an intermediary, brokering transactions for and among itself and the occupants of the other sides of the platform. The consumers provide personal information and advertisers pay the website/intermediary for access to the Plaintiff's and Class Members' information. The website's so-called "free" offerings are inducements to increase consumer participation, which, in turn, the website parlays into increased advertising revenue.

43. Because, as alleged herein, Defendants engaged in undisclosed and inadequately disclosed data collection from Plaintiff and Class Members, Plaintiff and Class Members did not receive the full value of the exchange. In essence, Defendants raised the price Plaintiff and Class Members paid to obtain Defendant's services by extracting an undisclosed premium in the form of Plaintiff's and Class Members' information.

44. Because Defendants impose an undisclosed cost on Plaintiff and Class Members by taking more information than they were entitled to take, Defendant's practices imposed economic costs on Plaintiff and Class Members.

45. In addition, the undisclosed privacy and information transfer consequences of Defendants' practices imposed costs in the form of the loss of the opportunity to have entered into value-for-value exchanges with *other* web publishers offering similar services and whose business practices better conformed to Plaintiff's expectations. This is because Plaintiff and Class Members use their personal information not only to acquire online offerings; they use it to acquire a better-value exchange by choosing among competing websites.

46. Plaintiff's and Class Members' information, which they use as an asset of economic value in the ways described above, has value as an asset in the information marketplace. Online websites have proven the value of Plaintiff's and Class Members' information through those websites' own business models, such as the fact that an online website acquires revenue by providing consumer data to ad-

delivery entities, or by allowing such entities to access consumers and acquire their information online. These practices have created an active market in which consumer information has a discernable value.

47. Thus, Defendants' conduct alleged in this complaint constituted an ongoing course of conduct that harmed Plaintiff and Class Members, and caused them to incur financial losses, in that Defendants, without authorization, acquired the personal information of Plaintiff and Class Members, which information has economic value to Plaintiff and Class Members, causing them to incur costs in the form of information taken and opportunity costs in the form of uses of the economic value of their information of which Defendant deprived them.

48. Defendants used Plaintiff's personal information for its own economic benefit and realized significant economic benefits from the conduct described above; Defendants' purpose in acquiring Plaintiff's and Class Members' data was to advance its commercial interests.

49. Defendants deprived consumers of their right to make adequately informed decisions about whether they would do business with Defendants or one of their competitors.

50. By that same conduct, Defendants imposed on consumers the undisclosed opportunity costs of their choosing to do business with Defendants.

51. The costs and harms described above are aggravated by Defendants' continued retention and commercial use of the improperly acquired consumer data.

52. Defendants' conduct caused economic loss to Plaintiff and Class Members in that, as discussed above, their personal information has discernable value, both to Defendants and to Plaintiff.

53. Defendants deprived Plaintiff and Class Members of and/or diminished the economic value of their personal information.

54. In addition to dispossessing Plaintiff and Class Members of the value of their personal information, Defendant dispossessed Plaintiff and Class Members of the value of their computers and computer-related services, as detailed below.

55. Consumers pay for computers capable of a particular level of processing speed.

56. Consumers pay for internet connectivity services of a particular level of transmission speed.

57. Defendants' undisclosed and unauthorized transmissions to Plaintiff and Class Members' computers usurped computer and connectivity resources to which Defendants were not entitled, diminishing the performance of Plaintiff's and Class Members' computer processing and connectivity.

58. Defendant's actions caused diminutions in processing and connectivity performance because, not only were their actions undisclosed and unexpected, their methods of information collection were more resource-intensive than expected, cookie-based or other routinely employed and reasonably-expected collection methods. Defendants' use of supercookies involved the transfer of larger files than cookies.

59. Plaintiff's experience is typical of the experiences of Class Members.

60. The aggregated loss and damage sustained by the Class, as defined herein, includes economic loss with an aggregated value of at least $5,000 during a one-year period.

61. Defendants, through the same act, perpetrated the acts and omissions set forth in this complaint through the deployment and iterative operation of the computer processes set forth above.

62. Plaintiff and Class Members have been harmed by Defendants' deceptive acquisition of their personal information in the loss of their rights to use, share, and maintain the confidentiality of their information, each according to his or her own discretion.

63. Plaintiff's and Class Members privacy interests have been invaded and or diminished by Defendants' outrageous and egregious conduct in taking personal information that does not belong to them and selling it to third parties.

III. CLASS ALLEGATIONS

64. Pursuant to the Federal Rules of Civil Procedure 23(a), (b)(l), (b)(2), and (b)(3), Plaintiff brings this action as a class action on behalf of himself and all others similarly situated as members of the Classes, defined as follows:

> "Verizon Supercookie Tracking Class": All individuals in the United States on whose computers or other mobile devices Defendant(s) stored supercookies for Defendant(s)' or others' use in place of or as backups for cookies.

> "Video Disclosure Class": All individuals in the United States who, during the Class Period, whose identified requests for specific video materials and/or services were disclosed to third parties without such individuals' express written consent.
>
> "Mississippi Sub-Class": All individuals residing in Mississippi whose Web browser privacy controls prevented or limited Defendant(s)' persistent storage and use of cookies and on whose computers Defendants stored supercookies.

65. Excluded from the Classes are Defendants, their legal representatives, assigns, and successors, and any entities in which Defendants have controlling interests. Also excluded are the judge to whom this case is assigned and the judge's immediate family.

66. The "Class Period" is January 1, 2012 to the present.

67. Plaintiff and Class Members reserve the right to revise these definitions of the Classes based on facts learned in the course of litigating this matter.

68. The Classes consist of millions of individuals and other entities, making joinder impractical.

69. The claims of Plaintiff are typical of the claims of all other Class Members.

70. Plaintiff will fairly and adequately represent the interests of the other Class Members. Plaintiff has retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiff and her counsel are committed to prosecuting this action vigorously on behalf of Class Members and have the financial resources to do so. Neither Plaintiff nor her counsel has any interests adverse to those of the other Class Members.

71. Absent a class action, most Class Members would find the cost of litigating their claims to be prohibitive and would have no effective remedy.

72. The class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation in that it conserves the resources of the courts and the litigants, and promotes consistency and efficiency of adjudication.

73. Defendants have acted and failed to act on grounds generally applicable to Plaintiff and other Class Members, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members.

74. The factual and legal bases of Defendants' liability to Plaintiff and other Class Members are the same, resulting in injury to Plaintiff and all of the other Class Members. Plaintiff and other Class Members have all suffered harm and damages as a result of Defendants' wrongful conduct.

75. There are many questions of law and fact common to Plaintiff and the Class Members and those questions predominate over any questions that may affect individual Class Members. Common questions for the Class include, but are not limited to the following:

a. whether Defendant(s) circumvented Class Members' browser controls through Defendants' use of supercookies;

b. whether Defendant(s) disclosed identified video-viewing details to third parties without Class Members' express, written consent;

c. whether Defendant(s) violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030;

d. whether Defendant(s) committed other violations of common law;

e. whether Defendant(s) misappropriated valuable information assets of Class Members;

f. whether Defendant(s) created or caused or facilitated the creation of personally-identifiable consumer profiles of Class Members;

g. whether Defendant(s) continue to retain and/or make use of, through supercookies, valuable information assets from and about Class Members;

h. what uses of such information were exercised and continue to be exercised by Defendant(s);

i. whether Defendant invaded the privacy interests of Class Members;

j. whether Defendant(s)' actions constituted trespass to personal property;

k. whether Defendant(s) have been unjustly enriched.

96. The questions of law and fact common to Class Members predominate over any questions affecting only individual members,

and a class action is superior to all other available methods for the fair and efficient adjudication of this controversy.

IV. CLAIMS FOR RELIEF

97. Based on the foregoing allegations, Plaintiff's claims for relief include the following:

FIRST CLAIM FOR RELIEF

Violations of the Computer Fraud and Abuse Act, 18 U.S.C § 1030, *et seq.*

98. Plaintiff incorporates the above allegations by reference as if fully set forth herein.

99. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, referred to as "'CFAA," regulates fraud and related activity in connection with computers, and makes it unlawful to intentionally access a computer used for interstate commerce or communication, without authorization or by exceeding authorized access to such a computer, thereby obtaining information from such a protected computer, within the meaning of 18 U.S.C. § 1030(a)(2)(C).

100. Defendant(s) violated 18 U.S.C. § 1030 by intentionally accessing Plaintiff's and Class Members' computers without authorization or by exceeding authorization, thereby obtaining information from such a protected computer.

101. The CFAA, 18 U.S.C. § 1030(g), provides a civil cause of action to any person who suffers damage or loss by reason of a violation of CFAA.

102. The CFAA, 18 U.S.C. § 1030(a)(5)(A) makes it unlawful to knowingly cause the transmission of a program, information, code, or command and as a result of such conduct, intentionally cause damage without authorization, to a protected computer , or a loss to one or more persons during any one-year period aggregating at least $5,000 in value.

103. Plaintiff's Class Members computers each constitute a "protected computer ... which is used in interstate

commerce and/or communication" within the meaning of 18 U.S.C. § 1030(e)(2)(B).

104. Defendant(s) violated 18 U.S.C. § 1030(a)(5)(A) by knowingly causing the transmission of a program, information, code, and command to be downloaded to and activated on Plaintiff's and Class Members' computers, which are protected computers as defined above; by storing and using supercookies to access, collect, and transmit details of Plaintiff's and Class Members' web activities and communications, Defendant(s) intentionally caused damage without authorization to those Class Members' computers by impairing the integrity of the computers.

105. Defendant(s) violated 18 U.S.C. § 1030(a)(5)(B) by intentionally accessing Plaintiff's and Class Members' protected computers without authorization, and as a result of such conduct, recklessly caused damage to Plaintiff's and Class Members computers by impairing the integrity of data and/or system and/or information

106. Defendant(s) violated 18 U.S.C. § 1030(a)(5)(C) by intentionally accessing Plaintiff's and Class Members' protected computers without authorization, and as a result of such conduct, causing damage and loss to Plaintiff and Class Members.

107. Plaintiff and Class Members suffered damage by reason of these violations, as defined in 18 U.S.C. 1030(e)(8), by the "impairment to the integrity or availability of data, a program, a system or information."

108. Plaintiff and Class Members have suffered loss by reason of these violations, including, without limitation, violation of the right of privacy, and disclosure of personal information that is otherwise private, confidential, and not of public record.

109. As a direct and proximate result of Defendant(s)' conduct, Plaintiff and Class Members have suffered harms and losses that include those described above.

110. Defendant(s)' unlawful access to Plaintiff's and Class Members' computers through the use of supercookies constituted

a single act that resulted in an aggregated loss to Plaintiff and the Class of at least $5,000 within a one-year period.

111. Therefore, Plaintiff and the Class are entitled to compensatory damages.

112. Defendant(s)' unlawful access to Plaintiff's and Class Members' computers and personal information has caused Plaintiff and Class Members irreparable injury. Unless restrained and enjoined, Defendant(s) will continue to commit such acts. Plaintiff's and Class Members' remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Plaintiff and Class Members to remedies including injunctive relief as provided by 18 U.S.C. § 1030(g).

SECOND CLAIM FOR RELIEF

Fraud

113. Plaintiff incorporates the above allegations by reference as if fully set forth herein.

114. Defendant(s)' actions alleged herein constitute unlawful, unfair, deceptive, and fraudulent business practices.

115. Defendant(s)' conduct constitutes acts, uses and/or employment by and/or their agents or employees of deception, fraud, unconscionable and unfair commercial practices, false pretenses, false promises, misrepresentations and/or the knowing concealment, suppression, and/or omission of material facts with the intent that others rely upon such concealment, suppression or omission, and as a consequence thereof suffer harm.

116. Defendant(s)' conduct was materially misleading in that (a) consumers reasonably expected that their browser, privacy and security controls would in fact control the kinds of tracking and profiling performed by Defendant(s); (b) consumers reasonably expected that, subject to their controls, any information collection would be performed through the use of cookies or other generally accepted data collection mechanisms, and not through technologies such as supercookies that by their very nature were designed to operate outside Plaintiff's and Class Members' expectations, awareness and ability to detect; (c) the very fact that consumers

had implemented privacy and security controls demonstrates the materiality of Defendant(s)' misrepresentations and omissions, through their actions, and through their data collection and use; (d) Defendant(s)' very use of such detection evading technologies demonstrates Defendant(s)' own recognition of the materiality of its own misrepresentations and omissions inasmuch as if their practices were material to consumers, Defendant(s) would not have gone to such lengths to hide them. The materiality of Defendant(s)' misrepresentations and omissions assumes even greater weight in light of the fact that not only did Defendant(s) thwart Plaintiff's and Class Member's expectations and express limitations, Defendant(s)' purpose, which Defendant(s) consistently achieved, was to iteratively and surreptitiously take Plaintiff's and Class Members' personal information, which was of value to them.

118. The unfair and deceptive trade acts and practices of Defendant(s) have directly, foreseeably, and proximately caused damages and injury to Plaintiff and other members of the Class.

119. Defendant(s)' acts and omissions, including misrepresentations, have caused harm to Plaintiff and Class Members in that they have suffered the loss of privacy through the exposure of the personal and private information and evasion of privacy controls on their computers as described more fully above.

120. Plaintiff seeks actual, compensatory, and punitive damages, costs and expenses, pre and post-judgment interest, and attorneys' fees.

THIRD CLAIM FOR RELIEF

Violation of Electronic Communications Privacy Act TITLE 18 UNITED STATES CODE, SECTION 2710, *ET SEQ.* (VIDEO PRIVACY PROTECTION ACT) (On Behalf of Plaintiff and the Video Disclosure Class)

121. Plaintiff and Class Members incorporate the above allegations by reference as if fully set forth herein. Defendant(s) are and were throughout the Class Period engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or

delivery of prerecorded video cassette tapes or similar audio visual materials in that Defendant(s) offered to online consumers prerecorded video programs, including previously released and posted, and originally developed news, entertainment, educational, and general interest video programs, and so was, throughout the Class Period, a video tape service provider as defined in the Video Privacy Protection Act.

122. Plaintiff and Class Members were users, renters, purchasers, and/or subscribers of goods and/or services from Defendant(s) and so were consumers as defined in the Video Privacy Protection Act.

123. As set forth above, Defendant(s) knowingly and without Plaintiff and Class Members' consent disclosed Plaintiff's and Class Members' identified video selections, knowing such disclosure included the disclosure of personally identifying information of Plaintiff and Class Members and their requests for and/or obtaining of specific video materials and/or services from Defendant.

124. Defendant(s)' actions were therefore in violation of the Video Privacy Protection Act, 18 U.S.C. §2710(b)(l).

125. Plaintiff and Class Members, as to each of them, are entitled to $2,500 in liquidated damages.

126. Plaintiff and Class Members are entitled to equitable relief that includes Defendant(s)' cessation of the conduct alleged herein.

127. Plaintiff and Class Members are entitled to equitable relief that includes an accounting of what records regarding their video materials requests and services were disclosed and to whom.

128. Plaintiff and Class Members are entitled to equitable relief that includes an accounting of Defendant(s)' compliance with 18 U.S.C. §2710(e), regarding the destruction of personally-identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected.

129. Plaintiff and Class Members seek punitive damages.

130. Plaintiff and Class Members are entitled to reasonable attorneys' fees and other litigation costs reasonably incurred.

131. Plaintiff and Class Members request such other preliminary and equitable relief as the Court deems appropriate.

FOURTH CLAIM FOR RELIEF
Trespass to Personal Property/Chattels

132. Plaintiff incorporates the above allegations by reference as if fully set forth herein.

133. By engaging in the acts alleged in this Complaint, Defendant(s) intentionally, and without justification or consent, physically interfered with the use and enjoyment of personal property in Plaintiff's and Class Members' possession, thereby causing harm to Plaintiff and Class Members.

134. Plaintiff and Class Members, at all times relevant to this action, were the owners and/or possessors of computers and of their information collected through Defendant(s)' use of supercookies placed on Plaintiff's and Class Member's computers.

135. Defendant(s) dispossessed Plaintiff and Class Members of the use of their computers, or parts of them, for a substantial time by commandeering those resources for their own purposes.

136. Defendant(s) dispossessed Plaintiff and Class Members of the value of their personal information by using tracking technologies to access such information.

137. Defendant(s) impaired the condition, quality, and value of Plaintiff's and Class Members' computers by the installation and use of supercookies, which constituted an ongoing alteration to Plaintiff's and Class Members' computers and which affected the performance of their browsers on an ongoing basis, circumventing Plaintiff's and Class Members' browser privacy controls and causing Plaintiff's and Class Members' browsers to transmit information to Defendant(s) to which Defendant(s) were not entitled.

138. Plaintiff and Class Members each had and have a legally protected economic interest in their personal information.

139. Plaintiff and Class Members sustained harm as a result of Defendant(s)' actions as described above.

140. Without Plaintiff's and Class Members' consent, or in excess of any consent given, Defendant(s) knowingly and intentionally accessed Plaintiff's and Class Members' property and caused injury to Plaintiff and the Members of the Class.

146. Defendant(s) engaged in deception and concealment in order to gain access to Plaintiff's and Class Members' computers and personal information.

147. Defendant(s)' installation and operation of the supercookies interfered and/or intermeddled with Plaintiff's and Class Members' computers, including by circumventing their controls designed to prevent the information collection effected by Defendant(s). Such use, interference and/or intermeddling was without consent, or in the alternative, in excess of consent.

148. Defendant(s)' installation and operation of the supercookies impaired the condition and value of Plaintiff's and Class Members' computers.

149. Defendant(s)' trespass to chattels, nuisance, and interference caused real and substantial damage to Plaintiff and Class Members.

150. As a direct and proximate result of Defendant(s)' trespass to chattels, nuisance, interference and unauthorized access of and intermeddling with Plaintiff's and Class Member's property, Defendant(s) have injured and impaired in the condition and value of Class Members' computers.

151. Plaintiff and Class Members have no adequate remedy at law.

152. Plaintiff, individually and on behalf of the Class, seeks injunctive relief restraining Defendant(s) from committing trespass to chattels, to purge the data, and damages.

DEMAND FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, prays for judgment against Defendant and that the Court may:

A. certify this case as a Class action on behalf of the Classes defined above, appoint Plaintiff as Class representative, and appoint Plaintiff's counsel as Class counsel;

B. declare that Defendant(s)' actions, as set forth above, violate the Computer Fraud and Abuse Act; the Video Privacy Protection Act; and such other claims and common law torts as are alleged above;

C. award injunctive and equitable relief as applicable to the Class *mutatis mutandis,* including:

i. prohibiting Defendant(s) from engaging in the acts alleged above;

ii. requiring Defendant(s) to provide reasonable notice and choice to consumers regarding Defendant(s)' data collection, profiling, merger, and de-anonymization activities;

iii. requiring Defendant(s) to disgorge to Plaintiff and Class Members or to whomever the Court deems appropriate all of Defendant(s) ill-gotten gains;

iv. requiring Defendant(s) to delete all data from and about Plaintiff and Class Members that it collected and/or acquired from third parties through the acts alleged above;

v. requiring Defendant(s) to provide Plaintiff and other Class Members reasonable means to decline, permanently, participation in Defendant(s)' collection of data from and about them;

vi. awarding Plaintiff and Class Members full restitution of all benefits wrongfully acquired by Defendant(s) through the wrongful conduct alleged above; and

vii. ordering an accounting and constructive trust to be imposed on the data from and about Plaintiff and Class Members and on funds or other assets

obtained by unlawful means as alleged above, to avoid dissipation, fraudulent transfers, and/or concealment of such assets by Defendant(s);

D. award damages, including statutory and treble damages where applicable, to Plaintiff and Class Members in an amount to be determined at trial;

E. award restitution against Defendant(s) for all money to which Plaintiff and the Classes are entitled in equity;

F. restrain, by preliminary and permanent injunction, Defendant, its officers, agents, servants, employees, and attorneys, and those participating with them in active concert, from identifying Plaintiff and Class Members online, whether by personal or pseudonymous identifiers, and from monitoring, accessing, collecting, transmitting, and merging with data from other sources any information from or about Plaintiff and Class Members;

G. award Plaintiff and the Class their reasonable litigation expenses and attorneys' fees; pre- and post-judgment interest to the extent allowable;

H. and such other relief as this Court deems just and proper.

JURY TRIAL DEMAND

Plaintiff hereby demands a trial by jury of all issues so triable.

The Plaintiff requests any other relief, either general or special, to which they may be entitled in the premises.

This the 4th day of February, 2015.

Respectfully submitted,

By: Bradley S. Clanton

Bradley S. Clanton (MS Bar No. 10505)
CLANTON LEGAL GROUP, PLLC
P.O. Box 4781
Jackson, Mississippi 39296
Direct: (601) 454-8794
Toll Free: (844) 425-2686
Facsimile: (866) 421-9918
Email: brad@clantonlegalgroup.com

Counsel for the Plaintiff